

Compte rendu

Ouvrage recensé :

CYNTHIA CHASSIGNEUX, *Vie privée et commerce électronique*, Montréal, Thémis, 2004, 348 p., ISBN 2-89400-184-3.

par Marc Lacoursière

Les Cahiers de droit, vol. 48, n° 3, 2007, p. 532-535.

Pour citer ce compte rendu, utiliser l'adresse suivante :

URI: <http://id.erudit.org/iderudit/043943ar>

DOI: 10.7202/043943ar

Note : les règles d'écriture des références bibliographiques peuvent varier selon les différents domaines du savoir.

Ce document est protégé par la loi sur le droit d'auteur. L'utilisation des services d'Érudit (y compris la reproduction) est assujettie à sa politique d'utilisation que vous pouvez consulter à l'URI <https://apropos.erudit.org/fr/usagers/politique-dutilisation/>

Érudit est un consortium interuniversitaire sans but lucratif composé de l'Université de Montréal, l'Université Laval et l'Université du Québec à Montréal. Il a pour mission la promotion et la valorisation de la recherche. Érudit offre des services d'édition numérique de documents scientifiques depuis 1998.

Pour communiquer avec les responsables d'Érudit : info@erudit.org

suite de processus qui permettent, après des débats larges et soigneusement documentés, d'en mesurer toutes les conséquences et d'en apprécier avec le maximum de justesse le bien-fondé.

Renée JOYAL

Université du Québec à Montréal

CYNTHIA CHASSIGNEUX, **Vie privée et commerce électronique**, Montréal, Thémis, 2004, 348 p., ISBN 2-89400-184-3.

Vu la facilité pour l'État de s'immiscer dans la vie privée par l'entremise des nouvelles technologies, George Orwell avait peut-être raison de craindre l'importance et la présence omnipotente de l'État en affirmant ceci : « Big Brother vous regarde¹ ». Ironiquement, certains affirment que le développement d'Internet exige une intervention étatique pour contrer les inquiétudes et les dérives de la protection des renseignements personnels et de la vie privée dans ce médium, bien que, aux yeux de plusieurs juristes, d'autres modes normatifs soient nécessaires, surtout en considérant la nature transfrontalière d'Internet. Cette question, qui a fait l'objet de plusieurs réflexions, a récemment été étudiée par une doctorante.

Dans son ouvrage *Vie privée et commerce électronique*, M^{me} Cynthia Chassigneux s'est interrogée sur la protection des renseignements personnels qui transitent dans Internet et, incidemment, sur la protection de la vie privée. Sa thèse s'inscrit dans une orientation purement positiviste, où elle aborde la question de l'encadrement des données personnelles selon l'angle de la protection par l'État et selon les « garanties complémentaires », soit un encadrement non étatique qui prend la forme de normes diverses. La coexistence de la régulation étatique et de ces normes est généralement acceptée de nos jours lorsqu'il s'agit de s'interroger sur la réglementation des activités dans Internet.

Lorsque Internet s'est démocratisé au milieu des années 90, cessant d'être l'apanage exclusif d'universitaires états-uniens et devenant accessible au grand public, les juristes se sont interrogés sur la qualification du réseau des réseaux et sur la manière de le réglementer. Alors qu'à ces débuts Internet était associé à une sorte d'espace non étatique, comme l'Antarctique, les tribunaux en sont venus à appliquer la législation existante aux activités cybernétiques. À cette époque se sont développées des règles et des normes de bienséance dans Internet, nommées « nétique », pour gouverner les relations entre les usagers, notamment en ce qui concernait les adeptes de groupes de discussion. Dès le début d'Internet, certains usagers ont outrepassé la nétique en lançant des attaques personnelles contre d'autres internautes². Peu à peu ont suivi d'autres problèmes liés non seulement à la diffamation, mais également à la fraude, que ce soit lors d'un achat, d'un paiement, ou en rapport aux données à caractère personnel.

Dans l'ensemble, la thèse de M^{me} Chassigneux est tout à fait pertinente eu égard aux problèmes soulevés par la protection des données personnelles. En effet, l'auteure explique fort bien les enjeux soulevés, les tentatives et les difficultés à résoudre les problèmes. Très largement documentée, sa thèse est, malheureusement, trop descriptive, car elle élude parfois le volet analytique.

En première partie, M^{me} Chassigneux s'intéresse à l'encadrement classique du traitement des données personnelles. Au titre I, le premier chapitre explique en détail les techniques de profilage par les commerçants. En particulier, l'auteure met bien en relief l'importance pour ceux-ci de cibler les tendances de magasinage en ligne, et surtout d'achat, des cybernautes. Plus précisément, les techniques de fichiers journaux et de fichiers de témoins (*cookies*), qui permettent

1. G. ORWELL, 1984, Londres, Secker and Warburg, 1949, p. 12.

2. E. KATSH, « Online Dispute Resolution: Some Implications for the Emergence of Law in Cyberspace », 2006 3(10) *Lex Electronica*, [En ligne], [www.lex-electronica.org/articles/v10-3/katsh.htm] (9 mars 2007).

le traitement invisible des données dans le but d'identifier l'utilisateur, y sont notamment examinées. M^{me} Chassigneux étudie par la suite la question de l'utilisation de ces profils par les commerçants, en particulier en matière de publicité. Les publicités dans Internet peuvent donc être adaptées aux internautes grâce au profil élaboré à leur insu. Dans une certaine mesure, ce profilage publicitaire au sujet de l'utilisateur peut être inoffensif ou, dans certains cas, lui être bénéfique. Le problème se pose sérieusement lorsque les données personnelles sont partagées entre le gestionnaire d'une vitrine Internet et une tierce personne. Comme le mentionne l'auteur, «[u]n tel traitement des renseignements collectés sur un site Web est licite si et seulement si l'internaute est préalablement informé par le commerçant électronique que les données communiquées pourront faire l'objet d'un partage³». Tel est l'esprit de la législation sur le sujet⁴. Après avoir expliqué le fonctionnement des transferts de données entre les sites, M^{me} Chassigneux aborde la qualification du statut juridique des données. Cette question, d'un grand intérêt et d'une pertinence certaine, ne serait-ce qu'en raison de la valeur économique de ces données, est malheureusement évacuée trop rapidement, l'auteur ne discutant que brièvement de deux décisions judiciaires.

Le second chapitre du premier titre I est consacré au thème de la confiance, qui constitue la pierre angulaire du commerce électronique. Ce concept est bien expliqué, à partir de son sens étymologique, en passant par son rôle social jusqu'à la «modélisation de la confiance», soit les protections légales et les garanties complémentaires. Dans ces derniers cas, ces aspects juridiques sont examinés respectivement au titre II et dans la seconde partie de l'ouvrage. Dans ces circonstances, la présentation de ces instruments juridiques peut sembler redondante.

Comme nous l'avons mentionné, le titre II étudie les protections juridiques. Le

premier chapitre, qui décrit les instruments juridiques, ainsi que leur analyse juridique, est très bien présenté. À titre d'exemple, il y est question des lignes directrices de l'Organisation de Coopération et de Développement Économiques (OCDE)⁵ qui ont eu une importance majeure dans le développement du commerce électronique et dans la protection des données personnelles. Comme l'indique l'auteur, ces lignes directrices «reconnaissent [...] la possibilité de recourir non seulement aux protections légales mais aussi aux garanties complémentaires mises en place par le marché⁶» pour traiter les données personnelles, si le gestionnaire du fichier respecte certains principes : limitation en matière de collecte de données, qualité des données, spécification des finalités, limitation de l'utilisation, garanties de sécurité, transparence, participation individuelle, responsabilité et flux transfrontalier de données. Ces principes fondamentaux se trouvent en général dans la plupart des instruments juridiques. Au Canada et au Québec, la *Loi sur la protection des renseignements personnels et les documents électroniques*⁷ et la *Loi sur la protection des renseignements personnels dans le secteur privé*⁸, qui complète les articles 35 à 41 du *Code civil du Québec*, s'inspirent également des lignes directrices de l'OCDE. Malgré la qualité de ces instruments, il faut convenir que leur mise en application demeure ardue. Ces difficultés d'application sont discutées par l'auteur dans la seconde partie de l'ouvrage, lorsqu'elle parle des garanties complémentaires. Enfin, l'auteur note, à juste titre, que les États-Unis n'ont pas légiféré sur la protection des

3. C. CHASSIGNEUX, *Vie privée et commerce électronique*, Montréal, Thémis, 2004, p. 54.

4. *Infra*, notes 7 et 8.

5. ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES (OCDE), *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel*, Paris, OCDE, 23 septembre 1980.

6. C. CHASSIGNEUX, *op. cit.*, note 3, p. 110.

7. *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5.

8. *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., c. P-39.1.

renseignements personnels dans le secteur privé (à l'exception de quelques domaines) et se sont contentés de n'englober que le secteur public.

Au deuxième chapitre est abordée la logique de certains principes fondamentaux, soit, dans un premier temps, le consentement à la divulgation des données et, dans un second temps, les étapes successives du traitement des données, c'est-à-dire de la collecte à la destruction. Rappelons que le consentement est l'élément clé de la protection des renseignements personnels. Sous réserve de quelques exceptions, il est essentiel à la collecte des données. Il va sans dire que le consentement doit être préalable, manifeste, libre, éclairé et donné à une fin spécifique. Le traitement des données, qui concerne la collecte, l'utilisation, la communication, la sécurité, l'exactitude et la destruction, est bien expliqué et analysé, l'auteure notant au passage les situations auxquelles ces principes se heurtent, notamment en ce qui concerne la collecte des renseignements nécessaires.

La seconde partie de l'ouvrage s'attarde à décrire l'encadrement actuel du traitement des données personnelles, c'est-à-dire les garanties complémentaires. Celles-ci concernent l'autoréglementation, la corégulation et la normativité technique. Les garanties de ce type sont destinées à combler certaines des lacunes causées par les protections légales, ces dernières étant plus efficaces sur un territoire donné que dans le cyberspace. Le titre I porte sur la teneur des garanties complémentaires, alors que le titre II discute de la valeur et de la portée de ces garanties.

En pratique, les garanties complémentaires peuvent prendre la forme de politiques de confidentialité ou de labels de qualité, ces deux caractéristiques étant discutées dans les deux premiers chapitres. Les gestionnaires de site Web doivent faire preuve de transparence dans la diffusion de l'information pour rehausser la confiance des internautes. En règle générale, la transparence se traduit par des politiques de confidentialité, lesquelles sont inspirées par les lignes directrices de l'OCDE, et apparaît sous la forme de contrats d'adhésion ou de clauses

annexes. La question fondamentale concerne la qualification de la nature de l'obligation d'information : obligation de moyen ou de résultat ? Bien que cette question soit abordée par l'auteure, la qualité de l'analyse gagnerait à être plus approfondie. Par la suite, M^{me} Chassigneux réfléchit sur le contenu des politiques de confidentialité, en prenant comme exemple réel la vitrine Internet de la FNAC (librairie, disquaire et marchand d'appareils électroniques très populaire en France). Au chapitre suivant, l'auteure explore les labels de qualité. Une discussion sur ces labels, également appelés « sceaux de certification », exige une analyse des autorités de certification et de la cryptographie asymétrique. Poussant plus avant son étude, de manière incomplète toutefois en ce qui concerne la nature de l'autorité de certification et les internautes, l'auteure insiste plus sur la responsabilité que sur la nature *per se*. En revanche, l'explication des labels est très bien présentée. Cette section se termine par quelques exemples de labellisation de sites Internet, comme TRUSTe et BBB Online. Le troisième chapitre du titre I porte sur une initiative d'encadrement de la protection des renseignements personnels, la Platform for Privacy Preferences (P3P)⁹. Comme pour les exemples cités précédemment, il s'agit d'un excellent cas d'analyse.

Le second titre de cette partie aborde la délicate question de la valeur et de la portée des garanties complémentaires. Bien que ces garanties soient intéressantes, sinon pertinentes, quelles en sont les limites ? Cette discussion débute par une excellente analyse

9. Le site Web précise que « The Platform for Privacy Preferences Project (P3P) enables Websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents. P3P user agents will allow users to be informed of site practices (in both machine – and human – readable formats) and to automate decision-making based on these practices when appropriate. Thus users need not read the privacy policies at every site they visit » : P3P, *What is P3P ?*, [En ligne], 2006, [www.w3.org/P3P] (1^{er} mars 2007).

des effets des garanties complémentaires. Les effets concrets et symboliques, immédiats et différés ainsi que voulus et non intentionnels permettent de saisir de manière appropriée la portée des garanties complémentaires et de leur valeur relativement au but recherché. À la suite de cette mise en contexte, l'auteure achève sa thèse par une analyse du contrôle et de la surveillance des garanties complémentaires. Dans ce cas, M^{me} Chassigneux a choisi de se pencher sur les fonctions dévolues aux instances publiques plutôt que de faire la simple description de ces autorités en indiquant leur statut et leur rôle. Tout en mettant l'accent sur la Commission nationale de l'informatique et des libertés (CNIL) et la Commission de l'accès à l'information (CAI), l'auteure examine les fonctions de surveillance, d'instruction et d'information qui constituent le cœur du rôle de ces organismes. Elle note avec justesse que la surveillance doit s'exercer à chaque instant, c'est-à-dire *a priori* et *a posteriori*, pour assurer le respect des principes fondamentaux¹⁰. Très descriptive, cette présentation n'en demeure pas moins fort pertinente. Enfin, ce dernier chapitre se termine par une description, trop courte, à notre avis, du contrôle par des associations privées.

En somme, la thèse de M^{me} Cynthia Chassigneux traite une question qui prend de plus en plus d'importance dans les nouvelles technologies. Le problème des vols d'identité, y compris les fausses cartes de crédit, devient un fléau de plus en plus important, en partie causé par le transfert non autorisé de données personnelles dans Internet. Malgré son aspect descriptif prononcé, la thèse de M^{me} Chassigneux constitue un ouvrage très bien structuré, d'une qualité remarquable, d'une profondeur notable quant à la recherche juridique et d'une grande pertinence. Nous recommandons donc cet ouvrage sans hésitation.

Marc LACOURSIÈRE
Université Laval

JEAN-PIERRE BÉLAND (dir.), **L'homme biotech : humain ou posthumain ?**, Québec, Les Presses de l'Université Laval, 2006, 314 p., ISBN 2-7637-8348-1.

Aujourd'hui, l'appartenance d'un individu au genre humain, preuve génétique à l'appui, ne présente guère de difficulté dans le domaine juridique. Qu'en sera-t-il pourtant de cette question et du destin de l'homme dans un avenir où le critère génétique traditionnel sera mis à l'épreuve par des pratiques biotechnologiques nouvelles ? Que penser de cette question sous un angle tant scientifique qu'éthique et social ?

L'ouvrage sous la direction de Jean-Pierre Béland, professeur d'éthique, de philosophie et de sciences sociales à l'Université du Québec à Chicoutimi, rassemble plusieurs essais fort intéressants sur ce thème complexe et emblématique. Cet ouvrage est issu d'un colloque interdisciplinaire et interuniversitaire qui s'est tenu lors du 73^e Congrès annuel de l'Association francophone pour le savoir (Acfas), à l'Université du Québec à Chicoutimi en 2005. Nous y trouvons des textes de scientifiques, de philosophes et d'éthiciens. Et, disons-le d'emblée, c'est un livre de qualité qui inaugure une réflexion élargie sur la question.

Dans l'introduction, le professeur Béland met l'accent sur la constatation que les biotechnologies – « thérapie génique, clonage, création de cellules souches, création des chimères humain-animal » (p. 1) – contribuent progressivement à une augmentation vertigineuse des possibilités de modification de l'humain et à la transformation du corps de ce dernier en récepteur¹, destinataire, privilégié des objets technologiques. Ce qui relance, bien entendu, chez tous les auteurs, des interrogations par rapport aux théories humanistes et posthumanistes : « l'homme

1. Cf. G. VIDAL, *Corps récepteur et producteur dans les dispositifs multimédias. Plaisirs et contraintes face aux technologies multimédias*, Colloque « Médiations du corps », Université Stendhal-Grenoble 3/Gresec, 24-25 novembre 2000, [En ligne], 2003, [www.u-grenoble3.fr/stendhal/recherche/centres/mediations.html] (12 mai 2007).

10. C. CHASSIGNEUX, *op. cit.*, note 3, p. 285.